In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism

H. Brian Holland[*]

I. INTRODUCTION

In the ten years since its enactment, § 230[1] of the Communications Decency Act of 1996 ("CDA")[2] has become perhaps the single most significant statute in the regulation of online content, and one of the most heavily criticized. Many early commentators criticized both Congress, for its apparent inability to craft the more limited statute it intended, and the courts, for interpreting the statute broadly and failing to limit its reach. Later commentators focus more clearly on policy concerns, contending that the failure to impose liability on intermediaries fails to effectuate principles of efficiency and cost avoidance.

This Article takes the opposing view, in defense of broad § 230 immunity. It argues that the immunity provisions of § 230 play a significant role in broader questions of Internet governance. Specifically, § 230 immunity provides a means of working within the sovereign legal system to effectuate many of the goals, ideals, and realities of the Internet exceptionalism, cyberlibertarian movements. By mitigating the imposition of certain external legal norms in the online environment, § 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism. With the impact of external norms diminished, Web 2.0 communities, such as wikis and social networks, have emerged to facilitate a limited market in norms and values and to provide internal enforcement mechanisms that allow new communal norms to emerge. Section 230 plays a vital role in this

---

* Visiting Associate Professor of Law, Penn State University's Dickinson School of Law. I would like to express my appreciation to Professor Eric Goldman for his comments on an earlier draft of this article, and to reference librarian Jennifer Grieg and law student Laura Gebert for their research assistance. I owe a particular debt of gratitude to law student Kevin Wimberly, who served as my research assistant and editor for nearly three years. Finally, my appreciation to Sarah, Will and Ella for the most important things.

1. 47 U.S.C. § 230(c) (2000).

2. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 133–43.

process of building heterogeneous communities that encourage collaborative production and communication. Efforts to substantially reform or restrict § 230 immunity are therefore unnecessary and unwise.

Part II of this Article provides a brief introduction to § 230. As interpreted and applied by the judiciary, this statute is now conceived as a broad grant of immunity from tort liability, not only in terms of those who can claim its protection, but also in the breadth of predicate acts and causes of action to which such immunity extends. Part III of this Article attempts to position the expansion of § 230 immunity within the larger debate over Internet governance, suggesting that proponents of expanded immunity are successfully creating what might be characterized as a modified, less demanding form of cyberlibertarian exceptionalism. The dramatic expansion of § 230 immunity has in a limited sense effectuated a vision of a community in which norms of relationship, thought and expression are yet to be formed. The tort liability from which § 230 provides immunity is, together with contract, a primary means by which society defines civil wrongs actionable at law. In the near absence of these external norms of conduct regulating relationships among individuals, the online community is free to create its own norms, its own rules of conduct, or none at all. It is a glimpse of an emergent community existing within, rather than without, the sovereign legal system.

Part IV of this Article makes the case for preserving broad § 230 immunity. As an initial matter, many of the reforms offered by commentators are both unnecessary and unwise because the costs of imposing indirect liability on intermediaries are unreasonable in relationship to the harm deterred or remedied by doing so. Moreover, the imposition of liability would undermine the development of Web 2.0 communities as a form of modified exceptionalism that encourages the development of communal norms, efficient centers of collaborative production, and open forums for communication.

II. THE EXPANSION OF § 230 IMMUNITY

In May of 1995, a New York trial court rocked the emerging online industry with its decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*[3] The plaintiff in *Stratton* sought to hold the Prodigy computer network liable for libelous comments posted on one of its bulletin boards

3. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, *as recognized in* Dimeo v. Max, 433 F. Supp. 2d 523 (E.D. Pa. 2006).

by a third-party.[4] In its motion for summary judgment, the plaintiff argued that Prodigy was a "publisher" of the libelous comments, as opposed to a mere "distributor."[5] This was a key distinction, because under New York law—and the law of most states—publishers are held strictly liable for defamatory comments whereas distributors may be held liable only if they knew or had reason to know of the allegedly libelous nature of the material.[6]

In defense, Prodigy relied on *Cubby, Inc. v. CompuServe, Inc.*, a factually similar case in which the Southern District of New York ruled that the CompuServe computer network was to be treated as a distributor.[7] In reaching this conclusion, the court noted that CompuServe had "no opportunity to review" the libelous material before it was uploaded to the bulletin board and made immediately available to subscribers.[8] As such, "CompuServe ha[d] no more editorial control over such a publication than does a public library, book store . . . newsstand . . . [or] any other distributor."[9] As a distributor, CompuServe could only be liable if it "knew or had reason to know" that the comments were libelous.[10] Plaintiffs were unable to satisfy the knowledge requirement, and summary judgment was granted in favor of CompuServe.[11]

Despite the apparent similarities between the CompuServe and Prodigy bulletin board services, the New York state court rejected Prodigy's reliance on the *CompuServe* decision.[12] Distinguishing the cases factually, the *Prodigy* court agreed with the *CompuServe* court that the critical issue was whether Prodigy "exercised sufficient editorial control over its computer bulletin boards to render it a publisher with the same responsibilities as a newspaper."[13] In finding that Prodigy had,

---

4. *Id.* at *1.

5. *Id.* at *2.

6. *Id.* at *3.

7. 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991).

8. *Id.* at 137.

9. *Id.* at 140. The court also states "it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so." *Id.*

10. *Id.* at 140–41.

11. *Id.* at 141 ("Because CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements, summary judgment in favor of CompuServe on the libel claim is granted.").

12. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, *as recognized in* Dimeo v. Max, 433 F. Supp. 2d 523 (E.D. Pa. 2006).

13. *Id.* at *3.

unlike CompuServe, exercised sufficient editorial control, the court emphasized two key distinctions between the services, each related to Prodigy's positioning as a "family oriented computer network."[14] First, unlike CompuServe, Prodigy "held itself out to the public and its members as controlling the content of its computer bulletin boards."[15] Second, Prodigy exercised "editorial control" over its computer bulletin boards by "actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste.'"[16] Through these actions, Prodigy distinguished itself from CompuServe by "arrogat[ing] to itself the role of determining what is proper for its members to post and read on its bulletin boards."[17] As a result, Prodigy was treated as a publisher of the information and held strictly liable for the libelous comments of its third-party subscriber.[18]

Representatives of the online industry argued that the *Prodigy* decision placed service providers in an untenable position by "creat[ing] a 'Hobson's choice' between creating 'child safe' areas that expose the ISP to liability as an editor, monitor, or publisher, and doing nothing in order to protect the ISP from liability."[19] Congress responded to the decision by amending the CDA to include a tailored immunity provision addressing the online industry's concerns. As one element of what came to be known as the "Good Samaritan" provisions of the CDA,[20] § 230 was generally intended to provide online service providers and bulletin board hosts with immunity from tort liability for the defamatory acts of their users.[21] This was accomplished by addressing those specific elements of common law defamation at issue in the *CompuServe* and

14. *Id.* at *2.

15. *Id.* at *4.

16. *Id.*

17. *Id.*

18. *Id.*

19. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 62 (1996).

20. 47 U.S.C. § 230(c) (2000). *See* S. REP. No. 104-230, at 194 (1996) (Conf. Rep.) ("[T]his section provides 'Good Samaritan' protection from civil liability.").

21. *See* 47 U.S.C. § 230(c)(2) (providing that online service providers shall not be "treated as the publisher or speaker"). As described on Rep. Cox's website:

> Internet Freedom and Family Empowerment Act. Approved August 4, 1995, by 420-4 vote. Portions signed into law on February 8, 1996, as part of Telecommunications Act: Public Law 104-104. Ensures that on-line service providers who take steps to clean up the Internet are no longer subject to additional liability for being 'good samaritans.' Bars the Federal Communications Commission from content or economic regulation of the Internet.

Legislative Accomplishments: 104th Congress Legislative Accomplishments, *at* http://web.archive.org/web/20021128230716/cox.house.gov/html/accomplishments.cfm?id=74 (last visited Jan. 9, 2008).

Prodigy decisions—editorial control and the distinct treatment of publishers and distributors under the law. To that end, subsection (1) provided: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[22] Subsection (2) provided:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[23]

In the ten years following the enactment of § 230, courts consistently extended its application. This trend began in 1997 with the watershed decision in *Zeran v. America Online, Inc.*,[24] in which the Fourth Circuit applied § 230 to claims that America Online ("AOL") should be held liable for the defamatory content posted by one of its users.[25] The plaintiffs claimed liability arose in part because AOL had allegedly failed to remove third-party defamatory messages from its bulletin board

22. 47 U.S.C. § 230(c)(l).

23. *Id.* § 230(c)(2).

24. 129 F.3d 327 (4th Cir. 1997).

25. For reasons unknown, an anonymous AOL subscriber identified only as "KenZZ03" posted a message to one of AOL's bulletin boards titled "Naughty Oklahoma T-Shirts." Zeran v. America Online, Inc., 958 F.Supp. 1124, 1127 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997). The message advertised the sale of various "t-shirts with vulgar and offensive slogans related to the Oklahoma City [bombing] tragedy." *Id.* "Readers were invited to call 'Ken,' Zeran's first name, at Zeran's [actual] phone number." *Id.* At the time, Zeran had no knowledge of the posting and at no time was he involved in the sale of these t-shirts. *Id.* Not surprisingly, "Zeran was inundated with calls, most of which were derogatory and some of which included death threats and intimidation." *Id.* Zeran was "[u]nable to suspend or change his telephone number due to business necessity," so the offensive and threatening phone calls continued unabated. *Id.* The next day a second notice appeared under a slightly modified alias. *Id.* This notice announced that many shirts had "SOLD OUT," but that "several new slogans were now available." *Id.* Zeran's first name and telephone number were listed at the bottom of the message. *Id.* Making matters worse, an Oklahoma City radio station read one of the posts over the air and encouraged listeners to call "'Ken' at Zeran's telephone number to register their disgust and disapproval." *Id.* at 1128. Not surprisingly, this was followed by "another cascade of threatening, intimidating, any [sic] angry telephone calls." *Id.* This went on for weeks before finally tapering off. *Id.*

system within a reasonable time,[26] refused to post retractions to defamatory messages,[27] and failed to screen for similar defamatory messages thereafter.[28] The court found the plaintiff's tort claims were preempted by § 230, which rendered AOL immune.[29] In reaching this result, the court rejected a strict reading of § 230 as being limited to its terms. Specifically, although the statute failed to make any explicit reference to distributor liability, which the *CompuServe* and *Prodigy* decisions appeared to leave intact, the court read distributor immunity into the statute, finding that "distributor liability . . . is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230."[30] By collapsing the publisher-distributor distinction, the Fourth Circuit adopted the most expansive reading possible of both defamation law and § 230. Thus, even though AOL knew the statements were false, defamatory, and causing great injury, AOL could simply refuse to take proper remedial and preventative action without fear of liability.

Following *Zeran*, and building on that court's reading of both the statute and the policies sought to be effected, courts have consistently extended the reach of § 230 immunity along three lines: (1) by expanding the class who may claim its protections; (2) by limiting the class statutorily excluded from its protections; and (3) by expanding the causes of action from which immunity is provided. As to the first, courts have interpreted the provision of immunity to "interactive computer services" to include web hosting services,[31] email service providers,[32] commercial web sites like eBay[33] and Amazon,[34] individual[35] and company[36]

---

26. Zeran learned of the initial posting from a reporter investigating the story and immediately contacted AOL "to demand prompt removal of the notice and a retraction." *Id.* at 1127. "An AOL representative assured him that the offending notice would be removed." *Id.*

27. AOL refused to post a retraction on its network as "a matter of policy." *Id.*

28. After the second posting, Zeran demanded that "AOL delete the notice and take steps to block further bogus messages using his name and phone number." *Id.* AOL advised him that the notice would be deleted and that the account posting the notices would be terminated. *Id.* at 1127–28. Despite these assurances, similar notices continued to appear on AOL's bulletin board over the next week, with similar consequences. *Id.* at 1128.

29. *Id.* at 1136. *See also Zeran*, 129 F.3d at 334.

30. *Id.* at 332.

31. Does v. Franco Prods., No. 99 C 7885, 2000 WL 816779, at *4 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Does v. GTE Corp., 347 F.3d 655 (7th Cir. 2003). *See also* Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 412 (S.D.N.Y. 2001) (raised as a defense by web-hosting service, but held not dispositive).

32. Jane Doe One v. Oliver, 755 A.2d 1000, 1003–04 (Conn. Super. Ct. 2000), *aff'd*, 792 A.2d 911 (Conn. App. Ct. 2002).

33. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 712–14 (Cal. Ct. App. 2002); Stoner v. eBay Inc., No. 305666, 2000 WL 1705637, at *1 (Cal. Super. Ct. Nov. 1, 2000).

34. Schneider v. Amazon.com, Inc., 31 P.3d 37, 40 (Wash. Ct. App. 2001).

35. Sabbato v. Hardy, No. 2000CA00136, 2000 WL 33594542, at *3 (Ohio Ct. App. Dec. 18,

websites, Internet dating services,[37] privately-created chat rooms,[38] and Internet access points in copy centers[39] and libraries.[40] The additional provision of immunity to "users" of those services promises similar results. Already, one decision has held that a newsgroup "user" cannot be held liable for re-posting libelous comments by a third party,[41] while another court found a website message board to be both a provider *and* a user of an interactive computer service.[42]

The second line of extension results from a narrow reading of the term "information content provider," which defines the class for whom there is no immunity. Specifically, courts have held that those who make "minor alterations" or "take some affirmative steps to edit the material" provided by another do not become information content providers within the meaning of the statute so long as they retain the material's "basic form and message."[43] The third point of expansion has been to extend § 230 immunity beyond causes of action for defamation and related claims to provide immunity from claims of negligent assistance in the sale/distribution of child pornography,[44] negligent distribution of pornography of and to adults,[45] negligent posting of incorrect stock information,[46] sale of fraudulently autographed sports memorabilia,[47] invasion of privacy,[48] and misappropriation of the right of publicity.[49]

2000). *But see* Batzel v. Smith, No. CV 00-9590 SWW(AJWX), 2001 WL 1893843, at *8 (C.D. Cal. June 5, 2001) (holding that an individual website operator did not fall within the immunity provision of § 230 because the only "qualifying entities" under that provision are "true internet service providers, like America Online, that provide[] individuals with access to the internet").

36. Amway Corp. v. Proctor & Gamble Co., No. 1:98-CV-726, 1999 WL 33494857, at *4 (W.D. Mich. June 29, 1999) (Section 230 raised as a defense, but held not dispositive).

37. Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065–66 (C.D. Cal. 2002), *aff'd*, 339 F.3d 1119 (9th Cir. 2003).

38. Marczeski v. Law, 122 F. Supp. 2d 315, 327 (D. Conn. 2000).

39. PatentWizard, Inc. v. Kinko's, Inc., 163 F. Supp. 2d 1069, 1071 (D.S.D. 2001).

40. Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772, 776 (Cal. Ct. App. 2001).

41. Barrett v. Rosenthal, 146 P.3d 510, 527 (Cal. 2006). Interestingly, this case was originally misreported in practice journals as applying § 230 immunity to the host or operator of a chat room. However, the facts of the case indicate that the defendant was merely a user of the system. *Id.* at 527 (indicating that "Rosenthal used the Internet to gain access to newsgroups where she posted [an] article" by a third-party).

42. DiMeo v. Max, 433 F. Supp. 2d 523, 531 (E.D. Pa. 2006).

43. Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003). *See also* Donato v. Moldow, 865 A.2d 711, 724 (N.J. Super. Ct. App. Div. 2005) (quoting *Batzel v. Smith*).

44. Doe v. Am. Online, Inc., 783 So. 2d 1010, 1017 (Fla. 2001).

45. Does v. Franco Prods., No. 99 C 7885, 2000 WL 816779, at *5 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

46. Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).

47. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 715 (Cal. Ct. App. 2002).

48. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).

49. *See id.* at 1122, 1125 (extending § 230 immunity to defendant in claim "alleging invasion of privacy, misapproriation of the right of publicity, defamation and negligence"). *See also* Perfect

III. SECTION 230, INTERNET GOVERNANCE AND EXCEPTIONALISM

Situated within the larger debate over Internet governance, the concept of Internet exceptionalism presumes that cyberspace cannot be confined by physical borders or controlled by traditional sovereign governments, and thus that cyberlibertarian communities will emerge in which norms of relationship, thought and expression are yet to be formed. Although these ideas have been subjected to intense criticism and somewhat obscured by recent developments in the governance debates, they remain a touchstone for the cyberlibertarian ideal. This part of the Article seeks to clear space in the governance debates for this vision of exceptionalism, and argues that § 230 is in some limited way facilitating the emergence of cyberlibertarian communities in a modified, less demanding form.

A. Foundational Arguments of Internet Governance

The debate over Internet governance evolved in two surprisingly distinct, albeit convergent stages. The first stage of the governance debate focused on law and social norms, and whether these traditional models of regulating human relations could be validly applied to the online environment.[50] In this context, exceptionalism was conceptualized as a state of being to which the Internet had naturally evolved, apart from terrestrial space.[51] The second stage of the debate introduced network architecture as an important and potentially dominant means of regulating the online environment.[52] In this context, exceptionalism

---

10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118–19 (9th Cir. 2007) (finding that § 230 immunity extends to state-law intellectual property claims, including unfair competition, false advertising, and right of publicity).

50. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365 (2002); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) [hereinafter Goldsmith, *Against Cyberanarchy*]; Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998) [hereinafter Goldsmith, *The Internet*].

51. *See, e.g.*, John Perry Barlow, A Declaration of the Independence of Cyberspace, ¶ 2 (Feb. 8, 1996), http://homes.eff.org/~barlow/Declaration-Final.html (last visited Sept. 24, 2007) (declaring "the global social space we are building to be naturally independent of the tyrannies you seek to impose on us").

52. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 217 (1999). *See generally* David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, 52 STAN. L. REV. 1439 (2000). Interestingly, Lessig decided to use the wiki format to update his book as *Code 2.0*:

> After five years in print and five years of changes in law, technology, and the context in which they reside, *Code* needs an update. But rather than do this alone, Professor Lessig

became an objective to be pursued and protected as a matter of choice, rather than a natural state. At a more exacting level, these debates implicated fundamental questions of legitimacy, preference, politics, democracy, collective decision-making, and libertarian ideals.

In the early 1990s, as the Internet began to reach the masses with the advent of the World Wide Web,[53] a particular vision of the online environment emerged to advocate and defend Internet exceptionalism. Described by one scholar as "digital libertarianism,"[54] and another as "cyberlibertarian[ism],"[55] the vision was one of freedom, liberty, and self-regulation.[56] Cyberlibertarians believed the Internet could and would develop its own effective legal institutions through which rules would emerge.[57] These emerging norms would "play the role of law by defining legal personhood and property, resolving disputes, and crystallizing a collective conversation about online participants' core values."[58] As this account suggests, early cyberlibertarians tended to focus on norms of behavior, relationship, and content, rather than the control and regulation of network architecture. Control of architecture was seen almost exclusively as an instrument by which to enforce emerging social norms,[59] and not as a means of determining the norms

---

is using this wiki to open the editing process to all, to draw upon the creativity and knowledge of the community. This is an online, collaborative book update; a first of its kind.

Once the project nears completion, Professor Lessig will take the contents of this wiki and ready it for publication. The resulting book, *Code v.2*, will be published in late 2005 by Basic Books. All royalties, including the book advance, will be donated to Creative Commons.

WIKIHOME: WHAT'S GOING ON HERE?, http://codebook.jot.com/WikiHome (last visited Sept. 14, 2007).

53. *See* David T. Cox, *Litigating Child Pornography and Obscenity Cases in the Internet Age*, 4 J. TECH. L. & POL'Y 1, 5–6 (1999) ("[B]y 1994, the Internet was no longer a playground for only the academic and defense communities."). Cox further states "[p]re-Web Internet use required a certain computer savvy that few outside academia possessed. As the easy-to-use Web interface to the Internet grew, so did the Internet's popularity among the masses." *Id.* at 6.

54. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 177–79 (1997) (describing the "Internet Holy Trinity" of "digital libertarianism").

55. Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297 (1998) (describing "cyberlibertarians" and "anarcho-cyberlibertarians").

56. *See* Boyle, *supra* note 54, at 177–79.

57. *See* Johnson & Post, *supra* note 50, at 1387.

58. *Id.* at 1367.

59. *See id.* at 1388–89. Johnson and Post describe the connection between norms and enforcement in early cyberspace as follows:

Every system operator who dispenses a password imposes at least some requirements as conditions of continuing access, including paying bills on time or remaining a member of a group entitled to access (for example, students at a university). System operators

themselves. By the mid-1990s this process of self-regulation was well underway. As two leading cyberlibertarians observed in 1996, "[c]yberspace is anything but anarchic; its distinct rule sets are becoming more robust every day."[60]

At the same time, however, sovereign nations and their constituents increasingly sought to impose existing offline legal regimes on this emerging, resource-rich environment.[61] Many in the online community resisted, perceiving this regulation as a threat to the exceptional nature of the Internet.[62] Advocates of self-regulation envisioned cyberspace as a distinct sphere, apart from physical space.[63] These cyberlibertarian exceptionalists saw the imposition of existing offline legal systems grounded in territorially-based sovereignty as inappropriate.[64] They believed that the online environment should instead be permitted to develop its own discrete system of legal rules and regulatory processes.[65]

(sysops) have an extremely powerful enforcement tool at their disposal to enforce such rules—banishment. Moreover, communities of users have marshaled plenty of enforcement weapons to induce wrongdoers to comply with local conventions, such as rules against flaming, shunning, mailbombs, and more. And both sysops and users have begun to recognize explicitly that formulating and enforcing such rules should be a matter for principled discussion, not an act of will by whoever has control of the power switch.

While many of these new rules and customs apply only to specific, local areas of the global network, some standards apply through technical protocols on a nearly universal basis. And widespread agreement already exists about core principles of "netiquette" in mailing lists and discussion groups—although, admittedly, new users have a slow learning curve and the Net offers little formal "public education" regarding applicable norms. Moreover, dispute resolution mechanisms suited to this new environment also seem certain to prosper.

Id. (footnotes omitted).

60. *Id.* at 1389. *See also* Barlow, *supra* note 51, at ¶ 7 (asserting the rise of self-governance among the inhabitants of cyberspace, stating, "[w]here there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract [sic].").

61. *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 315–16 (2002) (describing the movement of nation-states "to regulate almost every conceivable online activity").

62. Johnson & Post, *supra* note 50, at 1378–87; Post, *supra* note 50, at 1367–71; Barlow, *supra* note 51, at ¶¶ 1–6.

63. *See, e.g.*, Johnson & Post, *supra* note 50, at 1400–01. Johnson and Post conclude:

Global electronic communications have created new spaces in which distinct rule sets will evolve. We can reconcile the new law created in this space with current territorially based legal systems by treating it as a distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self-regulatory processes, and entitled to appropriate deference—but also subject to limitations when it oversteps its appropriate sphere.

Id.

64. *See id.* at 1370–76 (claiming that the Internet, by its nature, destroys the link between territorial borders, sovereign nations, and legitimate control).

65. *See id.* at 1400–02 (discussing our ability to reconcile cyberlaw with legal systems created

As John Perry Barlow famously declared: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[66] Self-regulation was preferable in its own right because it had proven so effective in creating the environment sought to be preserved, and also because the alternative seemed devastating. The imposition of external, territorially-based legal regimes would be, the exceptionalists argued, infeasible, ineffective, and fundamentally damaging to the online environment.[67]

Faced with the attempted imposition of offline legal regimes, cyberlibertarians responded by attacking the validity of exercising sovereign authority and external control over cyberspace.[68] According to Professors Johnson and Post, two leading proponents of self-governance, external regulation of the online environment would be invalid because Internet exceptionalism—the state of being to which the Internet naturally evolved—destroys the link between territorially-based sovereigns and their validating principles of power, legitimacy, effect, and notice.[69] Most importantly, the Internet's decentralized architecture deprives territorially-based sovereigns of the power, or ability, to

---

by legitimate, self-regulatory processes entitled to deference but "subject to limitations when it oversteps its appropriate sphere").

66. Barlow, *supra* note 51, at ¶ 1.

67. *See id.* at ¶ 2 (declaring to the established sovereign powers that they "have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear").

68. *See* Johnson & Post, *supra* note 50, at 1375–76 (arguing that "the effects of online activities [are not] tied to geographically proximate locations"). *See also* Barlow, *supra* note 51, at ¶ 3 (asserting to established sovereign powers that "Cyberspace does not lie within your borders").

69. Johnson & Post, *supra* note 50, at 1370–76. Johnson and Post acknowledge the importance of territorial borders to the existing system of determining legal rights and responsibilities, and accept that this correlation makes sense in the off-line world. *Id.* at 1369–70. Such validity, according to Johnson and Post, is based on the logical relationship between territorial borders and four related considerations: power, legitimacy, effects, and notice. *Id.* The *power* to control a particular area of physical space, and the people and things located therein, "is a defining attribute of sovereignty and statehood." *Id.* at 1369. This power rests on the singular ability of the sovereign to enforce the law within its borders. *Id.* The *legitimacy* of sovereign power is, in turn, premised on the "consent of the governed"—the idea that "persons within a geographically defined border are the ultimate source of law-making authority for activities within that border." *Id.* at 1369–70. The exclusivity of sovereign power, to the exclusion of external forces, is rooted in the "relationship between physical proximity and the *effects* of any particular behavior[,]" at least where there is no substantial overlap. *Id.* at 1369 (emphasis added). Finally, as a practical matter, territorial borders serve as signposts giving *notice* that a new regulatory regime now applies. *Id.* at 1370. The Internet, Johnson and Post claim, by its nature destroys the link between territorial borders and these validating principles. *See id.* at 1370–76. ("[P]hysical borders no longer function as signposts informing individuals of the obligations assumed by entering into a new, legally significant place," because "[i]ndividuals are unaware of . . . those borders as they move through virtual space.").

regulate online activity.[70] Likewise, extraterritorial application of sovereign law fails to represent the consent of the governed,[71] or to effectuate exclusivity of authority based on a relative comparison of local effects.[72] The loss of these limiting principles results in overlapping and inconsistent regulation of the same activity with significant spillover effect.[73] Deprived of these validating principles, it would be illegitimate to apply sovereign authority and external control in cyberspace.

A primary challenge to these cyberlibertarian arguments came from Professor Goldsmith,[74] who engaged both their descriptive and normative aspects. In terms of the legitimacy of sovereign regulation, Goldsmith criticized Johnson and Post's limited view of sovereignty and over-reliance on the relationship between physical proximity and territorial effects.[75] Moreover, he argued that they had overstated the impossibility of regulation, mistaking ability for cost;[76] failed to recognize the deterrent effect on extraterritorial actors of local enforcement against end users and network components located within the territory;[77] and mistakenly equated valid regulation with some measure of near-perfect enforcement.[78] Finally, where true conflicts between sovereigns existed, Goldsmith argued that these could be resolved with the same tools used in the offline world—rules of jurisdiction, conflict of laws, enforcement, etc.[79] Throughout, Goldsmith struck at Johnson and Post's exceptionalist view of the Internet, implicitly rejecting the ultimate significance of both the technical and communal aspects of that ideal. This critique proved devastating to these early cyberlibertarian arguments.[80]

The governance debate entered its second phase in 1999 with the publication of Professor Lessig's book, *Code and Other Laws of*

---

70. *Id.* at 1370–73.

71. *See also* Barlow, *supra* note 51, at ¶ 3 (asserting that "[g]overnments derive their just powers from the consent of the governed . . . [and] [y]ou have neither solicited nor received ours").

72. *See* Johnson & Post, *supra* note 50, at 1375.

73. *See id.* at 1374.

74. *See generally* Goldsmith, *Against Cyberanarchy*, *supra* note 50; Goldsmith, *The Internet*, *supra* note 50.

75. Goldsmith, *Against Cyberanarchy*, *supra* note 50, at 1239–40; Goldsmith, *The Internet*, *supra* note 50, at 476–77.

76. Goldsmith, *The Internet*, *supra* note 50, at 478–79.

77. *Id.* at 481–82.

78. *Id.* at 478–83.

79. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 50, at 1232–37.

80. *See* H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1, 4–13 (2005) (describing the debates "on the governance of cyberspace, borders, and territorial sovereignty" between Professors Johnson, Post and Goldsmith, and weaknesses in the approach taken by Johnson and Post).

Cyberspace.[81] Prior to Lessig's book, the governance debate had focused primarily on behavioral and property norms, with the assumption that either existing sovereign law or the law emerging from Internet self-governance would prevail. Network architecture merely provided the means to enforce these norms,[82] particularly those emerging from self-governance.[83] Lessig reconceived Internet exceptionalism as a two-part phenomenon, one regulatory and the other cultural. The former recognizes that many of those features that make the Internet "exceptional" (in the cyberlibertarian sense) are merely coding choices, and not the innate nature of cyberspace.[84] Within the network, architecture and code are the most basic forms of regulation.[85] Code can be easily changed.[86] Thus, Lessig argued, to protect the cultural aspects of exceptionalism, we must first recognize the exceptional regulatory power of architecture and code within cyberspace, and its pivotal role in preserving or destroying that culture.[87]

Lessig first pointed out that law and social norms are but two means of regulating human behavior.[88] In cyberspace, unlike real space, it is possible for architecture to dominate regulatory structures.[89] Architecture acts as a regulator in the offline world as well—in the form of time, nature, physics, etc.—but our laws and social norms are generally conceived with these regulators assumed.[90] Alteration of that architecture is unusually difficult if not practically impossible. In cyberspace, by comparison, architecture in the form of code is remarkably fluid.[91] Code effectuates a series of choices, and code can be changed:

> Cyberspace . . . has different architectures . . . . An extraordinary amount of control can be built into the environment . . . . What data can be collected, what anonymity is possible, what access is granted,

---

81. *See* LESSIG, *supra* note 52.

82. *See* Barlow, *supra* note 51, at ¶ 10 (arguing that, for inhabitants of cyberspace, "[o]ur identities have no bodies, so, unlike you, we cannot obtain order by physical coercion").

83. *See id.* ("[F]rom ethics, enlightened self-interest, and the commonweal, our governance will emerge.").

84. *See* LESSIG, *supra* note 52, at 24, 27.

85. *Id.* at 27.

86. *See id.* (arguing that the difference between regulable and unregulable networks is "a matter of code" that "could be transformed").

87. *Id.* at 30.

88. *See id.* at 6 (stating that laws regulate real space and code regulates cyberspace).

89. *Id.*

90. *Id.*

91. *Id.* at 58–60.

> what speech will be heard—all these are choices, not "facts." All these are designed, not found.[92]

As this passage suggests, not only is code fluid, but within cyberspace it is a uniquely powerful form of regulation. Rather than regulating behavior and relationships through punishment, deterrence and post-violation corrective action, code provides the means to exercise perfect control and thus perfect regulation—regulation not just of effects, but of the very universe of choices from which an individual actor is able to select.[93]

With this shift in focus, the debate itself evolved. Lessig cautioned that the greatest threat to the exceptional culture of cyberspace comes from the union of perfect control and market forces of commerce.[94] The architectual components that provide the means of perfect control are held almost exclusively by private entitites with commercial and political interests distinct from the collective.[95] The "invisible hand," Lessig argued, cannot resist the promise of perfect control, and has little or no motivation to protect the fundamental values promoted by cyberlibertarian exceptionalism.[96] According to the cyberlibertarian narrative, barriers that are present in the real world do not exist or are *de minimus* in the online environment. In the context of Internet architecture, exceptionalism can be found in original principles of network design[97] that rely on open protocols and non-discriminatory data

---

92. *Id.* at 217.

93. *See id.* at 90–95 (arguing that code can be used indirectly by different "regulators" to constrain individual behaviors).

94. *See id.* at 30–60 (stating that "the changes that make commerce possible are also changes that will make regulation easy").

95. *Id.* at 217.

96. *See id.* at 6 ("The invisible hand, through commerce, is constructing an architecture that perfects control—an architecture that makes possible highly efficient regulation.").

97. *See* Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783, 1789 (2002). Lessig describes it this way:

> At the core of the Internet's design is an ideal called "end-to-end" (e2e) . . . [which contemplates networks designed] so that intelligence rests in the ends, and the network itself remains simple. Simple networks, smart applications.
>
> The reason for this design was simple . . . . New content or new applications could run regardless of whether the network knew about them. New content or new applications would run because the network simply took packets of data and moved them along. The fundamental feature of this network design was neutrality among packets. The network was simple, or "stupid," in David Isenberg's sense, and the consequence of stupidity, at least among computers, is the inability to discriminate . . . . [T]his network was architected never to allow anyone to decide what would be allowed.

Id. (citations omitted).

transfer[98]—a network that is decentralized, borderless, and with the potential for nearly unlimited data capacity. Indeed, the digital data flowing through this system is itself exceptional, because it is easy to create and manipulate, easy to copy with no degradation in quality, and easy to access and distribute. In the context of online relationships, exceptionalism resides (at the very least) in the interactivity,[99] immediacy,[100] and potential scope of interaction,[101] as well as the opportunity for anonymity.[102] However, the very promise of perfect control is to eliminate many of these choices and the fundamental values they reflect as subservient to commercial goals. In cyberspace, control over coded architecture supplies the means for making this election.[103] Building on this assertion, Lessig argued that in order to protect fundamental values, decisions regarding architecture should emerge from the body politic and collective decision-making, rather than being concentrated in private actors.[104]

For many cyberlibertarians, Lessig's message presented great problems.[105] Although many had already abandoned the argument that the exercise of sovereign authority in cyberspace was normatively invalid, they had not given up (as a matter of preference) the vision of an emergent, self-governed, digital libertarian space.[106] Sovereign legal

---

98. *Id.*

99. *See* Stephen R. Bergerson, *E-Commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527, 1530 (2001) (noting "[t]he intimate nature, immediacy, interactivity and popularity of online transactions").

100. *See id. See also* Jason Kay, *Sexuality, Live Without a Net: Regulating Obscenity and Indecency on the Global Network*, 4 S. CAL. INTERDISC. L.J. 355, 385 (1995) (noting that "[t]he Internet is unique as a communications entity due to both the size of its audience and the immediacy of communication between people.").

101. The "scope" of the Internet, as I use it here, refers simply to the vast, borderless nature of the network and its impact on online interactions. *See generally* Reno v. ACLU, 521 U.S. 844, 853 (1997) ("'Once a provider posts its content on the Internet, it cannot prevent that content from entering any community.'" (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996))).

102. *See* A. Michael Froomkin, *Anonymity and its Enmities*, 1995 J. ONLINE L. art. 4, ¶ 7, *available at* http://www.wm.edu/law/publications/jol/95_96/froomkin.html (observing that "[b]asically, anything you can do with words and pictures, you can do anonymously on the Internet"). *See also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 574–75 (1998) (describing areas of technology where anonymity exists); Mathias Strasser, *Beyond Napster: How the Law Might Respond to a Changing Internet Architecture*, 28 N. KY. L. REV. 660, 707–08 (2001) (describing peer-to-peer architecture, Freenet, and anonymous nodes).

103. *See* LESSIG, *supra* note 52, at 217 (stating that "[a]n extraordinary amount of control can be built into the environment" of cyberspace).

104. *See id.* at 222, 225–30 (discussing the need for greater and better democracy as a response to a changing cyberspace).

105. *See* Post, *supra* note 52, at 1439 (stating that "[a]s a normative call to arms, however, [Lessig's] book is somewhat less successful").

106. *See id.* at 1440 (stating that the market, and not government, will bring the greatest

regimes were still seen as the greatest threat to that vision.[107] Territorial governments should, the cyberlibertarians argued, simply leave cyberspace alone to flourish.[108] From this perspective, Lessig's arguments about the unique regulatory power of architecture and code in cyberspace were largely convincing. But his description of the corrupting influence of perfect control and concentrated private power, and particularly his call for government regulation to counteract those influences and preserve fundamental values, were difficult to square with most libertarian views. Professor Post articulated this position:

> Fundamental values are indeed at stake in the construction of cyberspace, but those values can best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. We don't need "a plan" but a multitude of plans from among which individuals can choose, and "the market," and not action by the global collective, is most likely to bring that plenitude to us.[109]

The current debate on net neutrality provides a glimpse of this division. The network layers model divides the Internet into at least four layers: content, applications, logical/code, and physical/infrastructure.[110] Many commentators, including Lessig, are concerned that the private owners that control the physical/infrastructure layer will, in pursuit of cross-layer vertical integration and increased revenues, "use their control of the 'last mile' of the network to block or slow access to content and applications that threaten their proprietary operations,"[111] or to place "toll booths at every on-ramp and exit on the information superhighway."[112] These fears have been crystallized by recent court rulings and FCC rule making that released broadband suppliers from prohibitions on discrimination between content and application providers, and the announcement by some of the broadband companies that such

---

protection).

107. *See id.* at 1458 (stating the author's skepticism of more political control over the regulation of cyberspace).

108. *See id.* at 1459 ("[C]yberspace needs architectures where deliberation and reason and freedom can flourish.").

109. *Id.* at 1440.

110. Adam Thierer, *Are "Dumb Pipe" Mandates Smart Public Policy? Vertical Integration, Net Neutrality, and the Network Layers Model*, 3 J. TELECOMM. & HIGH TECH. L. 275, 279 (2005).

111. Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 3 (2005) (summarizing Lessig's position).

112. Lawrence Lessig & Robert W. McChesney, *No Tolls on the Internet*, WASH. POST, June 8, 2006, at A23, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108_pf.html.

discrimination is imminent.[113] With Congress debating an overhaul of the Telecommunications Act, advocates of net neutrality are seeking its imposition by regulatory mandates[114] requiring, in general terms, that the infrastructure remain simple, "dumb pipes"[115] that treat all Internet content alike to be moved across the network at the same speed. This would in turn encourage broadband providers to remain confined to the physical/infrastructure layer and out of the content business, with less incentive to discriminate. According to Lessig, these governmentally-imposed regulatory mandates are necessary to protect "the simple but brilliant 'end-to-end' design of the Internet that has made it such a powerful force for economic and social good: All of the intelligence and control is held by producers and users, not the networks that connect them."[116]

The irony of this debate is readily apparent. Many who might otherwise have characterized themselves as cyberlibertarian, or at least sympathetic to the vision of the Internet as a unique and "powerful force for economic and social good"[117] in which existing norms might not apply and fundamental values could be reconceived as emerging from the community rather than established political institutions, are suddenly contradicting themselves. The norms and values of the online community, rather than emerging from the common, are both imposed by external sovereign legal systems and subordinated to the control of commercial entities. In the extremes, it seems to present a choice between entrenched political power and unregulated market forces, with neither providing adequate protection for individuals. Thus, many of the Internet exceptionalists who sought to segregate the Internet from territorial boundaries, who assumed existing sovereign governments and legal regimes were the greatest threat to the online community, who believed that the computer scientist would remain in control of the network (and thus in control of enforcement) found themselves asking Congress to protect the Internet from private actors and market forces.

---

113. *See* Thierer, *supra* note 110, at 283–85 (stating that "there are signs that the days of full-blown structural access may be numbered").

114. *See* Yoo, *supra* note 111, at 3–5 (stating that "network neutrality hearkens back to the regime of mandatory interconnection and interface standardization used so successfully by the courts and the FCC to foster competition in telephone equipment").

115. Thierer, *supra* note 110, at 276. Thierer describes the distinction between dumb pipes and intelligent networks as follows: "A purely dumb pipe, for example, would be a broadband network without any proprietary code, applications, or software included. An intelligent network, by contrast, would integrate some or all of those things into the system." *Id.*

116. Lessig & McChesney, *supra* note 112.

117. *Id.*

B. What Is Left of Exceptionalism?

What then is left of Internet exceptionalism? In his revolutionary "A Declaration of the Independence of Cyberspace," John Perry Barlow described cyberspace as consisting not of computers, wires, or code, but of "transactions, relationships, and thought itself."[118] It was this vision, this perception of an evolving "social space,"[119] that guided Barlow's ideal of the culture he sought to preserve—a distinct vision of potential worthy of protection. Barlow's expression of the basic cyberlibertarian norms that define that environment reflect his focus on behavior, relationship, and expression:

> We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.
>
> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.
>
> Your legal concepts of property, expression, identity, movement, and context do not apply to us.[120]

To many early inhabitants of cyberspace, communal control and regulation of network architecture appeared a given, if for no other reason than that perfect external control seemed almost impossible.[121] Freedom of choice in individual expression, human behavior, and relationships were the heart of the online cultural and social ideal that stirred Barlow and other cyberlibertarians.

As it evolved, the governance debate fractured this largely unified vision, distinguishing validity from preference, law and social norms from architecture and code, technical exceptionalism from cultural exceptionalism, government power from private commercial power, and even libertarian from libertarian. Lessig argued persuasively that the greatest threat to digital libertarianism arose from private actors, unbounded by fundamental values (including constitutional values) and

---

118. Barlow, *supra* note 51, at ¶ 6. Indeed, the very heart of Barlow's Declaration of Independence was a poetic rejection of these physical components. *See id.* at ¶ 1 (demanding "Governments of the Industrial world, you weary giants of flesh and steel . . . leave us alone").

119. *Id.* at ¶ 2.

120. *Id.* ¶¶ 7–9.

121. *See supra* text accompanying note 59.

with the ability to exercise perfect control over choice.[122] Lessig's analysis, generally speaking, was focused on the treatment of data as data, based primarily on the identity of its "owner" and the commercial interests represented.[123] Choice in action was to be controlled by the regulation of owned data,[124] discriminatory treatment of data to the benefit of certain owners, restriction of network access, and similar means.[125] These technical controls would then be bolstered by traditional sovereign law validating those measures.

What seems somewhat obscured in Lessig's architecture-and-code approach (which clearly remains the central concern of the governance debate) is Barlow's original vision of relational libertarianism, with its focus on expression of individual choice and the development of new communal social norms within a system of self-governance. This is the part of Internet exceptionalism that was, in a sense, overwhelmed by the debate over architecture and code. Yet there are some choices, primarily relational, that remain largely unaffected by that debate. In this sphere, the question is not access to choice, the ability to choose, or the available universe of choices, but rather what norms apply to the choices being made outside those controls.

Post argued that fundamental normative values could "best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values."[126] He believed that the imposition of sovereign legal regimes in cyberspace, rather than promoting fundamental values as Lessig argued, would instead deny the digital libertarian culture the opportunity to develop apart from the offline world, with its own set of fundamental values.[127] He argues it is better to serve the private interest (even if powerful and commercially motivated) than the interest of terrestrial sovereigns. Indeed, exceptionalism was seen as requiring self-governance, to the exclusion of external legal norms imposed by sovereign powers, as a precondition to the emergence of a new system of norms.

---

122. *See* LESSIG, *supra* note 52, at 217.

123. *See generally id.*

124. Such regulation includes expanded intellectual property rights, the contractual licensing of such rights rather than physical transfer of ownership, and digital rights management.

125. *See generally* LESSIG, *supra* note 52.

126. Post, *supra* note 52, at 1440.

127. *Id.*

C. Section 230 as a Form of CyberLibertarian Exceptionalism

Most would say that Barlow and Post lost the battle: that the mythical "civilization of the Mind," "immune to . . . sovereignty," in which "governance will emerge" anew to create and enforce new social norms[128] was just that—mythical. However, this particular strain of Internet exceptionalism, envisioned as self-governance and emerging social norms applicable to relationships between individuals (as opposed to data as data), has been preserved in a modified, less demanding form. Ironically, it is because of sovereign law, not in spite of it, that this occurred. The dramatic expansion of § 230 immunity has effectuated many of the ideals promoted by Post, Barlow, and others, albeit on a limited scale. This expansion has created an environment in which many of the norms and regulatory mechanisms present in the offline world are effectively inapplicable. This is so not because the very nature of cyberspace makes such application impossible, or because sovereign law is necessarily ineffective or invalid, but rather because sovereign law has affirmatively created that condition.

The torts for which § 230 provides immunity are, together with contract law, the primary means by which society defines civil wrongs actionable at law. These norms of conduct regulate relationships among individuals: articulating wrongs against the physical and psychic well-being of the person (e.g., assault, battery, emotional distress), wrongs against property (e.g., trespass to land, trespass to chattels, conversion), wrongs against economic interests (e.g., fraud, tortious interference), and wrongs against reputation and privacy (e.g., defamation, misappropriation of publicity, invasion of privacy).[129] As described in Part I of this Article, § 230 has been interpreted and applied to provide expansive immunity from tort liability for actions taken on or in conjunction with computer networks, including the Internet. Statutory language defining who may claim the protections of § 230 immunity, including "providers" of "interactive computer services" and the "users" of such services, has been broadly extended.[130] In contrast, the primary limitation on the range of claimants to § 230 immunity, which is statutorily unavailable to the allegedly tortious "information content provider," has been strictly construed.[131] Moreover, the immunity

128. Barlow, *supra* note 51, at ¶¶ 10, 15–16.

129. *See* WILLIAM L. PROSSER, LAW OF TORTS 2 (3d ed. West Publishing Co. 1964) (defining torts as civil wrongs).

130. *See supra* text accompanying notes 31–42.

131. *See supra* text accompanying note 43.

provided to this expansive cross-section of online participants now reaches well beyond defamation to include a wide range of other tortious conduct and claims.[132] As such, many of the norms of conduct regulating relationships among individuals in the offline world—those civil wrongs actionable at (tort) law—simply do not apply to many in the online world.

A few examples might provide the best illustration of this gap between offline societal norms as expressed in tort law and § 230 immunity from tort liability for online participants, even where the alleged civil wrong seems familiar to the offline community.

In Florida, a mother filed suit against AOL[133] alleging that one of its adult members had used AOL chat rooms to market child pornography, including photographs and videotapes depicting her eleven-year-old son engaged in sexual acts with other minors and the adult.[134] Although "complaints had been communicated to AOL as to [the member's] transmitting obscene and unlawful photographs or images and . . . AOL reserved the right to terminate without notice the service of any member who did not abide by its 'Terms of Service and Rules of the Road,' AOL neither warned [the member] to stop nor suspended his service."[135] Assuming for the purposes of AOL's motion to dismiss that the plaintiff had stated a cause of action for liability in negligence, the Florida Supreme Court nevertheless found AOL to be immune under § 230.[136]

In California, an individual filed suit against eBay alleging that eBay had actively "misrepresented the safety of purchasing items"[137] from third-party dealers, despite having general and constructive notice that these dealers were selling fraudulently autographed sports memorabilia.[138] Plaintiffs' claims were dismissed on the pleadings despite allegations that eBay had participated extensively in the disputed auction process, tightly regulated the transactions, retained the right to terminate the account of any seller engaged in fraudulent activity, and collected both placement and success fees when items were sold.[139] Moreover, eBay encouraged buyers to rely on its "star" safety system, which rates third-party sellers based on customer feedback.[140] Although

132. *See supra* text accompanying notes 44–49.
133. Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fla. 2001).
134. *Id.* at 1011–12.
135. *Id.* at 1012.
136. *Id.* at 1018.
137. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 717 (Ct. App. 2002).
138. *Id.* at 708.
139. *Id.*
140. *Id.* at 717.

eBay knew that these ratings were extensively manipulated by dealers—including those selling fake sports memorabilia—eBay continued to advertise that "[a] positive eBay rating is worth its weight in gold" to potential customers.[141] Under § 230, eBay was found to be entirely immune.[142]

In both of these cases, the defendant was alleged to be aware of the illegal acts of their users, and to be either actively facilitating those illegal acts or refusing to stop them, even where the defendants had the knowledge, technical ability, and contractual right to do so. In the offline world, such active and knowing facilitation would likely violate social norms established in tort law. In the online world, however, the defendants were immune from liability.[143] Established norms, as expressed through the mechanisms of tort law, were neutralized by § 230 and the courts' interpretations of that provision.

In the near absence of these external legal norms, at least within the range of choices being made outside the data-as-data architectural controls, the online community is free to create its own norms, its own rules of conduct, or none at all. The inhabitants may not have a blank slate—criminal law, intellectual property law, and contract law still apply[144]—but much of what Barlow embraced as central tenets (mind, identity, expression) remain undefined. It is a modified version of cyberlibertarian exceptionalism, less demanding of the sovereign and existing offline social norms, and therefore less satisfying. But it is nonetheless a glimpse of that society, maintained by the sovereign legal regime rather than against it. It now applies to nearly every tort that can be committed in cyberspace. It is nibbling at the edges of intellectual property rights. It protects against the civil liability components of

---

141. *Id.*

142. *Id.* at 719.

143. *See, e.g.*, Walter Pincus, *The Internet Paradox: Libel, Slander and the First Amendment in Cyberspace*, 2 GREEN BAG 2D 279, 279 (1999). Here, Pincus observes:

> I work under contract for the Washington Post Newspaper. If the Post published an article of mine defaming a private individual, the paper would be liable. However, if washingtonpost.com, the Post's on-line Internet site, were to carry the same article, it would not be similarly liable. Why? Because Section 230 of the Communications Decency Act of 1996 bars liability for interactive computer service providers exercising a publisher's traditional editorial functions, such as deciding whether to publish, withdraw, postpone, or alter content. The Act immunizes Internet providers from precisely the sort of liability on which plaintiffs rely to hold other publishers accountable.

Id.

144. 47 U.S.C. § 230(e)(1)–(4) (2000). *But see* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118–19 (9th Cir. 2007) (finding that § 230 immunity extends to state-law intellectual property claims, including unfair competition, false advertising, and right of publicity).

criminal acts. It extends to all but the first speaker, who may well get lost in the network to escape liability even without immunity.

IV. A CASE FOR PRESERVING § 230 IMMUNITY

As interpreted by the courts, the immunity provisions of § 230 have been heavily criticized. Many commentators have argued that by failing to impose indirect liability on intermediaries, significant harms will go undeterred or unremedied, and that § 230 should be reformed to serve the interests of efficiency and cost allocation. This part of the Article addresses these criticisms directly, concluding that substantially reforming the statute is both unnecessary and unwise because the cost of such liability is unreasonable in relation to the harm deterred or remedied. Indeed, given § 230's role in facilitating the development of Web 2.0 communities, in which a form of modified exceptionalism encourages "collaborative production" and the emergence of "non-commodified digital space that facilitates communication," reforming the statute to narrow the grant of immunity would significantly damage the online environment.[145]

A. Evaluating Calls for Reform

Early critics of § 230 tended to focus on the issues of congressional intent and broad interpretation by the courts.[146] More recent

---

145. *See* Mark Cooper, *From WiFi to Wikis and Open Source: The Political Economy of Collaborative Production in the Digital Information Age*, 5 J. TELECOMMS. & HIGH TECH. L. 125, 126–27 (2006) (calling collaborative product the next "main event").

146. In its initial phases, § 230 commentators tended to focus on the issue of congressional intent and the Fourth Circuit's decision in *Zeran v. America Online, Inc.*, discussed in Part I of this article. Most commentators strongly criticized the *Zeran* court's conclusion that the statute immunizes intermediaries not only from publisher liability for objectionable third-party content, but from distributor liability as well. This could not, most commentators agreed, be what Congress intended. As the principles outlined in *Zeran* nevertheless became widely accepted, criticism turned to new cases interpreting the statute to extend this expansive immunity both to a growing class of intermediaries and to a broadening range of wrongful acts. Few of these assessments moved significantly beyond the apparent inability of Congress to craft a statute effectuating its intent or the courts' inability (or unwillingness) to interpret the statute in a way that reasonably limited its impact. *See, e.g.*, Emily K. Fritts, Note, *Internet Libel and the Communications Decency Act: How the Courts Erroneously Interpreted Congressional Intent with Regard to Liability of Internet Service Providers*, 93 KY. L.J. 765, 767, 784 (2004/2005) (analyzing "how the courts have applied defamation law with regard to Internet Service Providers"); Miree Kim, *Narrowing the Definition of an Interactive Service Provider Under § 230 of the Communications Decency Act*, 2003 B.C. INTELL. PROP. & TECH. F. 033102 (2003), *available at* http://www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/2003033102.html (exploring why Congress's definition of internet service providers under § 230 is inadequate); Robert T. Langdon, Note, *The Communications Decency Act § 230: Make Sense? Or Nonsense?—A Private Person's Inability to*

commentators have moved beyond these issues to engage the larger implications of providing such sweeping immunity to online intermediaries, suggesting amendments to § 230 intended to effectuate policies of efficiency and cost allocation.[147] This critique begins with the premise that in the online environment individual bad actors are "typically far beyond the reach of conventional law."[148] This creates a situation in which significant individual harms cannot be legally deterred or remedied,[149] and the fear that "[w]ithout effective enforcement of consumer rights and remedies, the Internet will not fulfill its promise as a secure marketplace for procuring goods or services."[150] Given these negative conditions, where a third-party maintains a level of control that places it "in a good position to detect or deter another's bad act," the imposition of indirect liability is desirable.[151] The failure to do so may create inefficiencies by failing to detect and deter harmful behavior where the cost of doing so is reasonable. Commentators have argued that, in the online environment, intermediaries are in the best position to deter negative behavior, to track down primary wrongdoers, and to mitigate damages.[152] This is particularly true in regard to information-based torts, the damages of which might be mitigated in many circumstances simply by taking down, prohibiting, or blocking the objectionable content.[153] As the "least cost avoider,"[154] "ISPs might

---

Recover if Defamed in Cyberspace, 73 ST. JOHN'S L. REV. 829, 849–55 (1999) ("[T]he Communications Decency Act does a great disservice to private individuals harmed by defamation on the Internet by foreclosing adequate legal remedies."); Sewali K. Patel, Note, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 678–91 (2002) (discussing alternatives to existing interpretations of CDA immunity by courts and Congress).

147. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 226 (2006) (arguing "the goal [is] to encourage service providers to adopt the precautions that they can provide most efficiently while leaving any remaining precautions to other market actors"). *But see* Matthew Schruers, Note, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 264 (2002) ("[N]egligence and strict liability regimes fail to produce an efficient level of monitoring . . . [and] undermine the positive attributes of the Internet by producing a reductive effect on online speech and diminishing network effects [whereas,] [s]tanding in stark contrast to these results, the effect of Section 230 [immunity] . . . has been to create a relatively efficient regime that simultaneously preserves positive and prevents negative externalities.").

148. Lichtman & Posner, *supra* note 147, at 233.

149. Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 341 (2005).

150. *Id.* at 383.

151. Lichtman & Posner, *supra* note 147, at 230.

152. *E.g.*, Rustad & Koenig, *supra* note 149, at 385–86.

153. *Id.* at 339.

154. Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 249 (2005). Intermediaries are the least cost avoiders in the online context because of "(1) an increase in the likelihood that it will be easy to identify specific intermediaries for

rightly be held liable for permitting malicious behaviors that they could have detected or deterred at reasonable cost."[155]

At the heart of this attack on § 230 immunity is the idea that, in the absence of indirect intermediary liability, significant harms will go undeterred or unremedied. These fears are either misplaced or overstated. As an initial matter, it is not clear that a significant number of bad actors are beyond the reach of the law. Advances in technology are making it increasingly possible to locate and identify bad actors online, such that online anonymity is difficult to maintain.[156] Likewise, where the bad actor is identified but is found outside the jurisdiction, sovereign governments have developed methods for resolving disputes to permit the direct extraterritorial application of domestic law, such as rules of jurisdiction, conflicts of laws, and recognition of judgments.[157] Indeed, anti-exceptionalists have strenuously argued that the application of sovereign authority to online activity originating outside the jurisdiction is legitimate and valid in large part because of these rules.[158]

Moreover, although the immunity provided by § 230 arguably *mitigates* the legal incentives for online intermediaries to deter and remedy certain negative behavior, it does not eliminate those legal incentives. Section 230 expressly states that it has no effect on criminal law, intellectual property law, or communications privacy law.[159] These external norms remain applicable to and enforceable against both content-providers and intermediaries in the online environment. Perhaps even more significantly, although § 230 removes *legal* incentives to enforce the norms expressed in tort law, law is certainly not the only incentive for an intermediary to act. Communal, commercial and other incentives also play a role.[160] Indeed, § 230 immunity allows

large classes of transactions, (2) a reduction in information costs, which makes it easier for the intermediaries to monitor the conduct of end users, and (3) increased anonymity, which makes remedies against end users generally less effective." *Id.* at 240.

155. Lichtman & Posner, *supra* note 147, at 256.

156. *See, e.g.*, Katharine Q. Seelye, *Snared in the Web of a Wikipedia Liar*, N.Y. TIMES, Dec. 4, 2005, at 4-1 (stating that "Lawrence Lessig, a law professor at Stanford and an expert in the laws of cyberspace, said that contrary to popular belief, true defamation was easily pursued through the courts because almost everything on the Internet was traceable and subpoenas were not that hard to obtain. (For real anonymity, [Lessig] advised, use a pay phone.)").

157. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 50, at 1232–37 (describing tools to resolve true conflicts between sovereigns).

158. *Id.* at 1239–42.

159. 47 U.S.C. § 230(e) (2000).

160. *See* Jonathan A. Friedman & Francis M. Buono, *Limiting Tort Liability for Online Third-Party Content Under Section 230 of the Communications Act*, 52 FED. COMM. L.J. 647, 664 (2000) (arguing that "the concerns expressed by critics that *Zeran* would discourage [intermediaries] from monitoring their networks for offensive material have clearly proven to be incorrect"). *See also infra* notes 187–88 and accompanying text.

intermediaries the freedom to intervene in a multitude of ways. Thus, individual harms and marketplace security can be addressed through alternate legal regimes and internal incentives.

Furthermore, proponents of indirect intermediary liability concede that even where harms do exist, intermediaries may only rightly be held liable for failing to detect and deter harmful behavior where the cost of doing so is reasonable.[161] It is unclear, however, that the costs of intermedial regulation are reasonable. In terms of remedies and reforms, critics generally suggest some form of the detect-deter-mitigate model, imposing a duty upon the intermediary with the potential for liability in cases of breach.[162] The two most common models are "traditional damages regimes, [and] takedown damages schemes in which the offensive content must be removed after proper notice."[163] Proponents of traditional liability schemes generally find theoretical fault with the exceptionalist view of the Internet, and analytical fault with broad judicial interpretations of the statute that collapse "distributor with knowledge" liability into immunity from publisher liability.[164] Proponents of a "synchronized 'notice, takedown, and put-back' regime"[165] likewise work from a "distributor with knowledge" model that imposes a limited duty of care on intermediaries,[166] but generally acknowledge some degree of exceptionalism that requires a distinct scheme. Most suggest some variation utilizing elements of the Digital Millennium Copyright Act ("DMCA")[167] and the European Union's E-Commerce Directive, triggered by actual notice of the objectionable content or a standard of reasonable care, and requiring "prompt remedial action to avoid further losses."[168]

---

161. *See supra* note 155 and accompanying text.

162. *See, e.g.*, Rustad & Koenig, *supra* note 149, at 343–44, 389.

163. Mann & Belzley, *supra* note 154, at 251. Some commentators have suggested "'hot list' schemes in which the intermediary must avoid facilitation of transactions with certain parties." *Id.* at 250–51, 271–72. This approach, borrowed from the financial industry, shifts much of the burden from the intermediary to a third-party actor, usually the government, who acts to identify wrongdoers. *Id.* at 271. The intermediary would then play the purely ministerial role of blocking network transactions. *Id.*

164. *See* Melissa A. Troiano, *The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447, 1475–76 (2006). *See also* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 654 (2001) (arguing that under a comparative institutional analysis, the "legal rule of total immunity for intermediaries rather than distributor liability represents a failure of public policy and the poor resolution of a legal conflict").

165. Rustad & Koenig, *supra* note 149, at 389.

166. *Id.* at 388.

167. 17 U.S.C. § 1201(a)(1) (2000).

168. Rustad & Koenig, *supra* note 149, at 343–44, 389. It should be acknowledged that the fairly unique position of United States law with regards to intermediary immunity from liability for

The costs of these indirect intermediary liability schemes could be great. Under traditional liability rules, intermediaries may be forced to adopt a least-common-denominator approach, resulting in overly broad restrictions on expression and behavior. A modified distributor-with-knowledge approach, usually in the form of a takedown scheme similar to that employed by the DMCA, may produce the same type of chilling effect.[169] Indeed, a recent study found that the DMCA takedown provisions were "commonly being used . . . to create leverage in a competitive marketplace, to protect rights not given by copyright (or perhaps any other law), and to stifle criticism, commentary and fair use."[170] This is potentially exacerbated by the use of a "should have known" standard that can trigger the need to patrol for harmful content, raising costs and leading to even greater overbreadth in application.[171] Moreover, indirect liability reduces incentives to develop self-help

---

third-party content creates additional pressure for reform. *See generally* THE GLOBAL INTERNET POLICY INITIATIVE, APPLICATION OF DEFAMATION LAWS TO THE INTERNET (2001), *available at* http://www.internetpolicy.net/practices/libel_law.pdf (last visited Sept. 24, 2007) (discussing the applicable law of the European Union, the United Kingdom, Germany, etc.). Much of the Internet remains borderless and decentralized, with near universal access to data. *See* H. Brian Holland, *Inherently Dangerous: The Potential for an Internet-Specific Standard Restricting Speech that Performs a Teaching Function*, 39 U.S.F. L. REV. 353, 402, 403 n.242 (2005) (discussing "disquieting history of confronting perceived threats to our political system with laws that muffle voices of dissent"). In many cases, the effects of activities in cyberspace are felt simultaneously throughout the network. *See* Johnson & Post, *supra* note 50, at 1375 (describing the effects of online activity as being felt simultaneously throughout the network, "everywhere or nowhere in particular"). As a result, with each online act, content providers and their intermediaries are potentially exposed to multiple legal regimes, and thus overlapping and inconsistent regulation of the same activity. *See id.* at 1373–74 (discussing some states' assertion of "the right to regulate all online trade"). At the same time, multiple jurisdictions are exposed to the acts of individuals outside their borders with each act facilitated by intermediaries that have the potential ability to block those acts from entering the larger network. *See* Reno v. ACLU, 521 U.S. 844, 853 (1997) (quoting lower court which stated, "[o]nce a provider posts its content on the Internet, it cannot prevent that content from entering any community"); Joseph Kahn, *China Has World's Tightest Internet Censorship, Report Finds*, N.Y. TIMES, Dec. 4, 2002, at A13 (describing China's success in using routers as checkpoints to filter content in real time). In this context, distinctions between legal regimes are emphasized, particularly where complex and sensitive social norms and values are implicated.

169. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 683 (2006) (arguing that the DMCA's takedown procedures are overbroad); Mike Scott, Note, *Safe Harbors Under the Digital Millennium Copyright Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 99, 157 (2005/2006) (arguing that, as currently constructed, the DMCA was "tilt[ed] sharply in favor of the rights of copyright holders"). The Electronic Frontier Foundation has chronicled its legal campaign against a "DMCA abuser" who systematically used baseless takedown notices in an effort to censor speech. Electronic Frontier Foundation, Diehl v. Crook, http://www.eff.org/legal/cases/diehl_v_crook/ (last visited Sept. 24, 2007).

170. Urban & Quilter, *supra* note 169, at 687.

171. *See* Todd E. Reese, *Wading Through the Muddy Waters: The Courts' Misapplication of Section 512(c) of the Digital Millennium Copyright Act*, 34 SW. U. L. REV. 287, 300 (2004) (criticizing the common application of a "should have known" standard in the context of the DMCA).

technology, such as location or identity tracking software and user-end filters, the development of which was one of § 230's primary policy goals.[172] Thus, if the scale of undeterred or unremedied harms is minimal, and the negative impact of a detect-deter-mitigate model is significant, then the cost associated with the imposition of indirect intermediary liability is not reasonable.

B. Resisting the Urge Toward Homogeny[173]

The case for preserving § 230 immunity begins by recasting intermediary immunity in terms of exceptionalism, self-governance and norms, because it is precisely the gap between the offline social norms expressed in tort law and the broad immunity provided to online participants that has led to the rather strong criticism of § 230. As a conceptual matter, communal enforcement presents the greatest challenge to effectuating some modified version of the exceptionalist ideal. When external legal norms are excluded, internal enforcement mechanisms facilitate the emergence of new communal norms to take their place. Much of the criticism of § 230 stems from the lack of legal enforcement that accompanies immunity, and the resulting inability to form new social norms to replace those of the sovereign. It is important to recognize, however, that Web 2.0[174] communities, such as wikis[175] and social networks,[176] represent a real and significant manifestation of the

---

172. *See* 47 U.S.C. § 230(b)(3)–(4) (2000) (describing the policies behind the enactment of § 230).

173. This reference to "homogeny" is drawn from a talk given by Professor Eric Goldman of Santa Clara University School of Law. Professor Goldman spoke about derivative liability at a conference at Michigan State University Law School. *See* Talk on 47 USC 230 at Michigan State, http://blog.ericgoldman.org/archives/2005/04/talk_on_47_usc.htm (discussing his upcoming presentation). He pointed to the "emergence of heterogeneous communities" as a policy benefit of § 230 immunity. *See* Michigan State Talk (April 2005), *available at* http://blog.ericgoldman.org/archives/msu230talkapr2005.pdf (Professor Goldman's notes for the talk).

174. "Web 2.0 is [a]n umbrella term for the second wave of the World Wide Web .... Sometimes called the 'New Internet,' Web 2.0 is not a specific technology; rather, it refers to two major paradigm shifts. The one most often touted is 'user-generated content ....' The second is 'thin client computing.'" TECHENCYCLOPEDIA: *Web 2.0*, http://www.techweb.com/encyclopedia/defineterm.jhtml;jsessionid=5WCZR4K4VZ5AQQSNDLRCKH0CJUNN2JVN?term=web+2.0 (last visited Jan. 9, 2008).

175. "A wiki is [a] Web site that can be quickly edited by its visitors with simple formatting rules." TECHENCYCLOPEDIA: *Wiki*, http://www.techweb.com/encyclopedia/defineterm.jhtml?Term=wiki (last visited Oct. 29, 2007).

176. "A Web site that provides a virtual community for people interested in a particular subject or just to 'hang out' together. Members communicate by voice, chat, instant message, videoconference and blogs, and the service typically provides a way for members to contact friends of other members .... [A] 'virtual community.'" TECHENCYCLOPEDIA: *Social Networking Site*, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=socialnetworkingsite (last visited

exceptionalist vision, because they both facilitate a market in norms and values, and provide the internal enforcement mechanisms necessary for internal norms to emerge. Section 230 plays a vital role in the development of these communities by substantially and continually mitigating the primacy of external legal norms within the confines of the community. This permits choice, empowers the intermediary to create a market in social norms, and allows alternate forms and gradations of enforcement. The architecture of the community gives these choices form and substance, backed by an enforcement model, such that communal norms have the opportunity to develop. In this sense, § 230 and the Web 2.0 model effectuate the emergence of a modified form of exceptionalism. The reforms proposed by most commentators would have a negative impact on these communities, with little benefit beyond those communal norms that are likely to emerge, and should be rejected.

1. Exceptionalism, Self-Governance and Social Norms

Exceptionalism does not argue for the absence of social norms. Instead, exceptionalism embraces the idea of cyberspace as an environment in which the authority of external legal regimes is minimal, and where an open market in norms and values works in concert with self-governance to permit the online community to establish its own substantive social norms. Section 230 helps to effectuate a modified form of exceptionalism by moderating the imposition of external legal norms so as to permit a limited range of choices—bounded, at least, by criminal law, intellectual property law and contract law—in which the online community is free to create its own norms and rules of conduct. However, the development of social norms within this environment requires not only the ability to exercise broad individual choice among different values and embodiments of those values, but also some mechanism of communal enforcement through which to effectuate some form of self-governance.

Early proponents of exceptionalism were able to focus on relational libertarian ideals, viewing the Internet as a unique social space in which norms governing thought, expression, identity, and relationship should be permitted to evolve. This focus developed precisely because the mechanisms of enforcement required for self-governance and the evolving definition of emergent social norms were taken for granted. The architecture of enforcement was primarily controlled by a

---

Apr. 3, 2007).

community involved in the process as adherents to the exceptionalist ideal, who could be trusted both to ensure broad individual choice and to utilize the means of enforcement as a tool of self-governance as norms emerged.[177]

As a means of effectuating exceptionalism, the primary weakness of § 230 is the lack of an enforcement component. Although the modified exceptionalism enabled by § 230 permits a range of choices, it does nothing to provide enforcement mechanisms to solidify emerging communal norms. Where immunity exists, legal enforcement mechanisms are never triggered. Likewise, the architecture of enforcement relied upon by early exceptionalists is no longer communal or likely committed to the vision of a distinct cyberlibertarian space, but is instead concentrated in private commercial entities. As a consequence, § 230 immunity creates a gap. Certain external legal norms are excluded, but internal communal norms are often unable to coalesce to take their place. It is this gap, resulting from the lack of architectural enforcement controls, which fuels criticism of the immunity provision. In application, however, an enforcement model has emerged that mediates the tension between the broad availability of individual value choices and the ability to effectively self-govern so as to permit the development of communal norms.

2. Communities of Modified Exceptionalism

Web 2.0 communities are, generally speaking, "a perceived second generation of web-based . . . services—such as social-networking sites, wikis and folksonomies—which aim to facilitate collaboration and sharing among users."[178] The community is structured as a limited commons and is built on an "architecture of participation"[179] that operates as a platform for user-created content and collaboration.[180] At its heart are principles of open communication, decentralized authority,

---

177. *See supra* note 59.

178. WIKIPEDIA: *Web 2.0*, http://en.wikipedia.org/wiki/Web_2 (last visited Apr. 3, 2007) (referencing and defining Web 2.0 as a phrase coined by O'Reilly Media in 2004). *See also* Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (last visited Sept. 24, 2007) (identifying, inter alia, Wikipedia and folksonomies such as del.icio.us and Flickr as examples of Web 2.0).

179. O'Reilly, *supra* note 178.

180. *Id. See also* Kevin Kelly, *We Are the Web*, WIRED, Aug. 2005, *available at* http://www.wired.com/wired/archive/13.08/tech.html (describing the promotion of consumers into producers and the future of the Internet as a "network of social creation" and a "community of collaborative interaction").

the freedom to share and re-use, and an idea of the Internet as a social forum or market for exchanging opinions and ideas in search of norms[181] to create a "culture based on sharing."[182] Section 230 plays a vital role in the development and maintenance of these architectures by providing intermediaries with limited immunity from liability for the tortious content provided by users.[183] Indeed, in this sense, § 230 seems to favor the development of Web 2.0 services and the provision of user-based content over the traditional model of providing first-party institutional content.

The parallels between Web 2.0 and Barlow's vision of a communal social space are evident, albeit in modified form. Barlow embraced the potential of an environment premised upon freedom of choice in individual expression, human behavior and relationships.[184] To achieve that potential, he and others believed that regulation by existing sovereign powers must be rejected in favor of self-governance, so that new communal social norms might have the opportunity to emerge.[185] At the heart of this ideal was an affirmation that values participation in the market of expression, ideas and action without the constraint of preconceived value judgments. Web 2.0 promises a somewhat limited version of this environment—existing within sovereign authority, narrowed by certain enduring norms, and confined to segmented communities administered by private entities—by facilitating the market by which norms are tested.

Two of the most common models of these Web 2.0 services, wikis and social networks, are indicative of how § 230 can effectuate the modified form of cyberlibertarian exceptionalism described above. Partly as a result of the immunity from liability provided by § 230, these services facilitate the market in social norms by creating enclaves in which users may exercise broad (although not unbounded) individual choice among values. At the same time, the intermediary retains control over the architecture and thus the means of enforcement. As the market defines social good through the evolution of communal norms, that architecture may be employed as a mechanism of governance.[186] In the absence of legal incentives, the enforcement of communal norms is

181. *See generally* O'Reilly, *supra* note 178; Kelly, *supra* note 180.

182. Kelly, *supra* note 180.

183. *See supra* Part II (describing the expansive immunity provided by § 230 as interpreted and applied by the courts).

184. *See supra* notes 118–20 and accompanying text.

185. *See supra* notes 55–59, 62–66 and accompanying text.

186. *See, e.g.*, *infra* notes 195–207 and accompanying text (describing the architectural enforcement mechanisms utilized by Wikipedia and the resulting development of social norms).

driven by internal incentives, such as the need for financial support from community donations, a communal desire for information integrity, or the need to build an audience for advertising.[187] In some communities, participants may be incentivized by credibility and stature in the form of temporal seniority, post count, rank within the community's governing body, etc.[188]

The online encyclopedia Wikipedia[189] is a specific example of a Web 2.0 community. Culturally, Wikipedia is a "massive experiment in collective action."[190] Each entry in the Wikipedia database is created and edited by volunteers[191] who are guided by three primary principles: the Neutral Point of View policy, the No Original Research policy, and the Verifiability policy.[192] Registered users can originate new articles, and any user, whether registered or anonymous, can edit an existing article.[193] In the period between Wikipedia's inception in January of 2001 and

187. Wikipedia is a project of the Wikimedia Foundation, Inc., a 501(c)(3) not-for-profit organization that relies significantly on donations from its users. Wikimedia: Fundraising, http://wikimediafoundation.org/wiki/Fundraising (last visited Apr. 3, 2007). Likewise, the Wikipedia community has developed enforcement mechanisms to further its internal norms of objective writing and accuracy. *See, e.g.*, *infra* note 205 (describing the Colbert "elephant" incident). In the commercial arena, intermediaries are motivated by economics to act responsibly and police their services. *See* Friedman & Buono, *supra* note 160, at 664–65. *See also* Cooper, *supra* note 145, at 126–27 (noting that commercial platforms, such as social networking sites, are driven more clearly by economic incentives).

188. The online service Experts Exchange provides an excellent example of this type of incentive. Experts Exchange: Home, http://www.experts-exchange.com/ (last visited Sept. 24, 2007). This website describes itself as one that uses collaborative knowledge to solve technology problems. Experts Exchange: About Us, http://www.experts-exchange.com/aboutUs.jsp (last visited Apr. 3, 2007). Contributors are incentivized by a community point system that rewards the best answers to technology questions, and by competing for awards such as "Expert of the Year." Experts Exchange: The Third Annual Expert Awards 2007, http://www.experts-exchange.com/expertAwards2007.jsp (last visited Apr. 3, 2007).

189. WIKIPEDIA, http://wikipedia.org/. Wikipedia describes itself as a "multilingual, web-based, free content encyclopedia project . . . written collaboratively by volunteers . . . ." WIKIPEDIA: *Wikipedia*, http://en.wikipedia.org/wiki/Wikipedia (last visited Apr. 3, 2007).

190. FERNANDA B. VIÉGAS ET AL., VISUAL COMM'N LAB, IBM RESEARCH, TALK BEFORE YOU TYPE: COORDINATION IN WIKIPEDIA § 2, http://www.research.ibm.com/visual/papers/wikipedia_coordination_final.pdf (last visited Sept. 24, 2007).

191. Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 164 (2006).

192. *Id.* at 169–70. *See also* WIKIPEDIA: *Policies and Guidelines*, http://en.wikipedia.org/wiki/Wikipedia:Policies_and_guidelines (last visited Jan. 9, 2008).

193. Myers, *supra* note 191, at 169. Prior to December 5, 2005, any user, registered or not, was able to create new articles. *Id.* at 171. However, after a particularly embarrassing incident in which an unregistered user wrote that John Seigenthaler, Sr. "was thought to have been directly involved in the Kennedy assassinations of both John, and his brother, Bobby," Wikipedia altered its architecture and policies to permit only registered users to create new articles. *Id.* at 170–71.

October of 2006, this experiment in voluntary collaborative action produced more than five million articles.[194]

These activities are overseen by two levels of administrators, "sysops" and "voting sysops."[195] "Sysops" have the power to edit pages, delete or undelete articles and article histories, protect pages, and block or unblock user accounts or IP addresses.[196] Voting sysops, or super administrators (also called "bureaucrats" or "stewards"), have the further power to create additional sysops with the approval of the community.[197] In February 2006, in response to a series of significant and persistent acts of vandalism,[198] the co-founder of Wikipedia created an additional layer of administration that permits a particular super administrator to protect or modify any article at the direction of the co-founder.[199] These administrators help facilitate dispute resolution and enforcement. Low-level disputes are resolved in "talk pages and other coordination spaces" that provide a "local, low-cost arena for resolving conflicts."[200] Here, moderators guide members to resolution with reference to policies and guidelines developed over the life of the community.[201] Thus, principle values and norms can lead to more specific rules. This approach works in most cases.[202] More serious violations, such as malicious editing of an article (or "vandalism"), are addressed through fast-repair mechanisms executed by community members.[203] In 2004, Wikipedia developed a new enforcement tool, page protection, to address repeated acts of vandalism.[204] Wikipedia administrators are also able to block user accounts or IP addresses.[205]

---

194. *Id.* at 167 (noting that of this number, approximately 1.4 million articles are in English).

195. *Id.* at 169.

196. *Id.*

197. *Id.*

198. In February 2007, Fuzzy Zoeller filed a lawsuit against a Miami consulting firm after he was able to track the computer that had added a defamatory paragraph to his biography on Wikipedia. Michael O'Keeffe, *The Score Hears . . . Fuzzy's Clear About Lawsuit*, N.Y. DAILY NEWS, Feb. 25, 2007, at 63. The entry concerning John Seigenthaler was traced to an employee of a Nashville delivery company. Seigenthaler said he would not take the prankster to court. Katharine Q. Seelye, *A Little Sleuthing Unmasks Writer of Wikipedia Prank*, N.Y. TIMES, Dec. 11, 2005, at 1–51.

199. Myers, *supra* note 191, at 171.

200. VIÉGAS ET AL., *supra* note 190, at § 2.

201. *Id.* at 5, 7.

202. *See id.* at 8 (noting that "[i]n all 25 pages coded for this paper, the overwhelming majority of requests for information were answered, strengthening the sense of a strong, supportive community.").

203. *Id.* at 3.

204. *Id.*

205. Myers, *supra* note 191, at 169. A simple example demonstrates how this system of norms, oversight and enforcement works. In August of 2006, television satirist Stephen Colbert coined the

As described, the Wikipedia community reflects a modified form of the exceptionalist model, allowing initially for individual choice among a range of values, facilitating a market in social norms, and providing a means of enforcement to effectuate norms as they develop. Indeed, recent studies reflect not only that norms have emerged from this market, but that those norms have solidified and expanded.[206] Through this process, the Wikipedia community is moving from an immediate focus on particular articles "to a more high-level concern for the quality of content and the health of the community."[207]

On the content side, Wikipedia has developed a "self-conscious social-norms-based dedication to objective writing,"[208] as well as norms of "formality and language standardization."[209] Not unexpectedly, open source projects such as Wikipedia are not immune to abuse.[210] In terms of community health, and to protect against these abuses, Wikipedia has adopted a code of conduct[211] and principles of etiquette that stress civility

---

word "wikiality" to describe the idea that "a large number of people could create a truth by consensus." John Kenney, *Elephant*, WIKIPEDIA, http://en.wikipedia.org/wiki/User:John_Kenney/Elephant_%28wikipedia_article%29 (last visited Sept. 24, 2007); Melissa P. McNamara, *Stephen Colbert Sparks Wiki War*, CBS NEWS, Aug. 9, 2006, http://www.cbsnews.com/stories/2006/08/08/blogophile/main1873436.shtml?source=RSSattr=Opinion:Blogophile_1873436 (last visited Sept. 24, 2007) (describing Colbert's "wikiality" as "[t]he idea . . . that if you convince enough people that something false is actually true, it ends up becoming accepted as the truth"). To test his theory, Colbert urged his viewers to "edit Wikipedia's 'elephant' article to indicate that the population of elephants had tripled in the last six months." Kenney, *supra*; McNamara, *supra*. When viewers responded by following Colbert's instructions, "Wikipedia editors swung into action, locking new and anonymous users out of the 'elephant' article, as well as the 'Stephen Colbert' article and several others." Kenney, *supra*. What followed was an online debate over the actions of Colbert, his viewers and the Wikipedia editors, through which the process of creating and modifying norms within that community continued. McNamara, *supra* (cataloging some of the online reactions).

206. *See* VIÉGAS ET AL., *supra* note 190, at abstract (concluding that the fastest growing areas of Wikipedia are devoted to coordination and organization, with an emphasis on strategic planning, group coordination, the development of policy and process, and the enforcement of guidelines and conventions).

207. *Id.* at § 4.

208. Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369, 386 (2002).

209. VIÉGAS ET AL., *supra* note 190, at § 2.

210. According to *The Washington Post*, "[p]ranksters have altered Wikipedia entries to say that Tony Blair's middle name is 'Whoop-de Do'; that David Beckham was a Chinese goalkeeper in the 18th century; that the golfer Fuzzy Zoeller had abused alcohol and drugs; and that John Seigenthaler, a respected journalist, was thought to be involved in the assassinations of both Kennedys (before absconding to the Soviet Union)." Cass R. Sunstein, *A Brave New Wikiworld*, WASH. POST, Feb. 24, 2007, at A19. *See also* Seelye, *supra* note 156, at 4-1 (quoting Jimmy Wales, the founder of Wikipedia (in response to the Seigenthaler episode), "[Wikipedia has] constant problems where we have people who are trying to repeatedly abuse our sites").

211. WIKIPEDIA: *Five Pillars*, http://en.wikipedia.org/wiki/Wikipedia:Five_pillars (describing the code of conduct as one of five pillars).

and discourage personal attacks.[212] As discussed above, these norms are enforced through an architecture that is designed to reinforce those norms with an eye towards the health of the community.[213] At the most basic level, "social norms coupled with a simple facility to allow any participant to edit out blatant opinion written by another in contravention of the social norms keep the group on track."[214] Over time, more complex mechanisms for dispute resolution and enforcement have developed, such that in the past few years the "administrative and coordinating elements" of Wikipedia have been "growing at a faster pace than the bulk of articles in the encyclopedia."[215]

The relationship between architecture and social norms is fascinatingly apparent in the recent development of Wikipedia Scanner,[216] "a searchable database that ties millions of anonymous Wikipedia edits to organizations where those edits apparently originated, by cross-referencing the edits with data on who owns the associated block of internet IP addresses."[217] An architectural choice by Wikipedia to track and correlate the IP address of any anonymous user who edits the encyclopedia[218] enabled a member of the Wikipedia community to create a monitoring mechanism for enforcing social norms, particularly the norm of neutrality, in more controversial areas.[219] In terms of more formal enforcement, some edits that previously may have been overlooked are now being reexamined in light of the organization from which they originated. Less formally, but perhaps even more effectively, organizations which are perceived to have breached the norms of the community have and will face recriminations.[220] Moreover, the entire

---

212. WIKIPEDIA: *Etiquette*, http://en.wikipedia.org/wiki/Wikipedia:Etiquette.

213. VIÉGAS ET AL., *supra* note 190, at § 6 (making the point that the community benefits when talk page moderators "turn[] the spotlight from the offending parties onto Wikipedia policies").

214. Benkler, *supra* note 208, at 387.

215. VIÉGAS ET AL., *supra* note 190, at § 1. *See also id.* at § 7 (noting the great "proportion of pages devoted to coordination and administration").

216. Virgil Griffith, Wikiscanner: List anonymous wikipedia edits from interesting organizations, http://wikiscanner.virgil.gr/ (last visited Sept. 24, 2007).

217. John Borland, *See Who's Editing Wikipedia—Diebold, the CIA, a Campaign*, WIRED, Aug. 14, 2007, *available at* http://www.wired.com/politics/onlinerights/news/2007/08/wiki_tracker (last visited Sept. 24, 2007). According to the article, Wikipedia Scanner was "the brainchild of Cal Tech computation and neural-systems graduate student Virgil Griffith . . . ." *Id.*

218. *Id.*

219. Virgil Griffith, the creator of Wikipedia Scanner, has noted: "Overall—especially for non-controversial topics—Wikipedia seems to work. For controversial topics, Wikipedia can be made more reliable through techniques like this one." Virgil Griffith, *WikiScanner FAQ*, http://virgil.gr/31.html (last visited Sept. 24, 2007).

220. *Wired* magazine, for example, created a submission page to find the "Most Shameful Wikipedia Spin Jobs." Kevin Poulson, *Vote on the Most Shameful Wikipedia Spin Jobs*, WIRED, Aug. 13, 2007, *available at* http://blog.wired.com/27bstroke6/2007/08/vote-on-the-top.html (last

community is now aware that enforcement of those norms is now more effective, presumably creating a deterrence effect.

The Wikipedia example illuminates a constant process, as choices are narrowed by communal norms that develop and are given life through enforcement mechanisms, such that principle norms generate a breadth of more particular rules.[221] Section 230 immunity plays an important role in this process, permitting the community to evolve and structure itself in the most efficient manner. To a limited extent, § 230 immunity permits uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. It further allows the intermediary to play an active role in facilitating the market in social norms and in creating enforcement mechanisms as a tool of self-governance. Those enforcement mechanisms can then themselves adapt. This allows not only for the development of distinct community values, but also for a means of tapping into incentives, adapting to evolving norms and conditions, and reducing costs associated with disputes. Within this framework, greater variations in community norms are possible. As communities grow, niche communities are formed at low cost. It is not the global vision of early exceptionalism, but rather a more limited and localized form of modified exceptionalism that functions as a laboratory for testing social norms and values.

V. CONCLUSION

Critics of § 230 have both overstated the harms arising from immunity and understated the costs of alternate schemes for imposing indirect liability on online intermediaries. At the same time, they have ignored the important role § 230 plays in the development of online communities. The immunity provided by § 230 helps to create the initial condition necessary for the development of a modified form of exceptionalism by mitigating the effect of external legal norms in the online environment. Web 2.0 communities are then able to facilitate a market in norms and provide the architectural enforcement mechanisms that give emerging norms substance. Given § 230's crucial role in this process, and the growing importance of Web 2.0 communities in which collaborative production is yielding remarkable results, reforming the statute to substantially narrow the grant of immunity is both unnecessary and unwise.

---

visited Jan. 9, 2008) (click on "submit your own sighting" hyperlink).

221. VIÉGAS ET AL., *supra* note 190, at § 1 (concluding that "Wikipedia is becoming less anarchic and more driven by policies and guidelines").